

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

IN RE: DEALER MANAGEMENT SYSTEMS
ANTITRUST LITIGATION

This Document Relates To:

All Actions

)
) MDL No. 2817
) Case No. 1:18-CV-00864
)

) Hon. Robert M. Dow, Jr.
) Hon. Jeffrey T. Gilbert, Magistrate
)

**MOTION FOR PARTIAL RECONSIDERATION OF [DKT. 441] ORDER ON MDL
PLAINTIFFS' OMNIBUS MOTION TO COMPEL**

I. Introduction

The Reynolds & Reynolds Company (“Reynolds”) is working diligently to comply with the Court’s November 19, 2018 Order. However, Reynolds respectfully requests that the Court reconsider its decision on one particular topic (“Reynolds’s Security Tools, Processes, and Training”) because it appears that the Court’s decision was based on a mistaken understanding of one aspect of the Plaintiffs’ allegations. Namely, the Court’s Order stated: “The security issue appears to be a central one in this case, and the documents Plaintiffs are seeking are relevant to an evaluation of Reynolds’s security rationale *for the change in the way it did business implemented in 2015.*” Order at 6 (emphasis added). Respectfully, no one has alleged that Reynolds changed the way it did business in 2015. To the contrary, Reynolds has unilaterally enforced a “closed system” policy for approximately the last decade. Plaintiffs’ allegation is that the defendants entered into a conspiracy in 2015 pursuant to which, among other things, CDK purportedly “closed” its DMS to third-party “data integrators.”

II. Reynolds’s security stance has been the same for at least the last decade.

The fact that Reynolds unilaterally disavowed and blocked hostile third-party access of its DMS long before the “conspiracy” alleged in this case is not in dispute. In its opinion vacating the preliminary injunction previously granted to Authenticom, the Seventh Circuit summarized:

Until 2015, the system furnished by CDK placed no restrictions on data harvesting by third-party integrators; Reynolds, in contrast, has always forbidden that practice in its system licenses. (The record indicates that the restriction in the Reynolds licenses did not stop Authenticom from persuading some Reynolds users to permit it to scrape data from them as well, in violation of their agreements with Reynolds.)

....

Despite the apparent preference of the dealers for the open model, CDK decided in 2015 to switch to a closed system.

Authenticom, Inc. v. CDK Global, LLC et al., 874 F.3d 1019, 1022 (7th Cir. 2017).

Likewise, in Judge St. Eve’s order granting in part and denying in part the defendants’ motion to dismiss Authenticom’s claims, the Court summarized the allegations as follows:

[I]n 2007, . . . Reynolds announced that it would start blocking data integrators from Reynolds DMSs. Since then, Reynolds has considered third-party, unauthorized scraping of its DMSs as “hostile access.” As a result of this policy change, Reynolds began disabling Authenticom’s credentials in 2009 by imposing “challenge questions” and “captcha” (entry requests to enter random or blurred text), which identify non-human users.

....

CDK, on the other hand, countenanced third-party access for far longer. Indeed, CDK touted its open architecture. . . . In 2015, however, CDK came to echo Reynolds’s disapproval of third-party access.

Dkt. 176 at 10-11. *See also* Consolidated Class Action Complaint (Dkt. 184) ¶ 7 (alleging that “starting in 2006, Reynolds took steps to block third party data integrators from accessing Reynolds DMS’s”); Authenticom Complaint (Dkt. 1, Case No. 1:18-cv-868) ¶ 92 (alleging that Reynolds began blocking hostile integrators “in earnest” in 2011).

In sum, Reynolds did not change its security stance in 2015 or any other time in the last decade.

III. Reconsideration is warranted with respect to this portion of the Court's Order.

In light of the above, the Court's Order appears to rely on a mistaken premise that the requests at issue are "relevant to an evaluation of Reynolds's security rationale for the change in the way it did business implemented in 2015." The Order also notes Plaintiffs' point that CDK reached an agreement with Plaintiffs regarding an identical request. Dkt. 441 at 6.

While it is unclear what weight the Court gave to CDK's agreement when making its decision with respect to Reynolds, we note again that Reynolds and CDK are differently situated with respect to the allegations regarding their system policies, so it should not be surprising that Reynolds was disinclined to agree to the same compromise as CDK.

In any event, in light of the apparent importance of the Court's statement that Reynolds changed its security policies in 2015, Reynolds respectfully requests that the Court reconsider its Order and deny the motion with respect to Issue #9 of Plaintiffs' Omnibus Motion to Compel.

In the alternative, in light of the broad and cumulative nature of this request as worded,¹ Reynolds would respectfully request that the Court modify its Order with respect to Issue #9 so that Reynolds's obligations are more clearly defined and narrowly tailored to the Court's remaining concerns (if any) after taking into account the fact that Reynolds is not alleged to have changed its policies.

IV. Statement of Compliance with Local Rule 37.2

Pursuant to Local Rule 37.2, Reynolds certifies that they have met and conferred with Plaintiffs' counsel in a good faith attempt to resolve the issue presented by this motion—namely by telephone conference on November 30, 2018. The participants included Brian Ross for

¹ By way of example only, Plaintiffs' "narrowed" requests asked for documents "regarding training for software developers working on Reynolds's DMS or integration programs"—a category that on its face goes well beyond security.

Reynolds, Michael Nemelka for the Individual Plaintiffs, and John Hughes and Matthew Kupillas
for the Dealer Class Plaintiffs.

Dated: December 3, 2018

Respectfully submitted,

/s/ Aundrea K. Gulley
Aundrea K. Gulley
Kathy D. Patrick
Brian T. Ross
Brice A. Wilkinson
Ross M. MacDonald
GIBBS & BRUNS LLP
1100 Louisiana Street, Suite 5300
Houston, TX 77002
(713) 650-8805
agulley@gibbsbruns.com
kpatrick@gibbsbruns.com
bross@gibbsbruns.com
bwilkinson@gibbsbruns.com
rmacdonald@gibbsbruns.com

Michael P.A. Cohen
SHEPPARD MULLIN RICHTER &
HAMPTON, LLP
2099 Pennsylvania Ave., NW, Suite
100
Washington, DC 20006
(202) 747-1900
mcohen@sheppardmullin.com

Leo D. Caseria
SHEPPARD MULLIN RICHTER &
HAMPTON, LLP
333 S. Hope St., 43rd Floor
Los Angeles, CA 90071
(213) 617-4206
lcaseria@sheppardmullin.com

*Counsel for Defendant The Reynolds
and Reynolds Company*

CERTIFICATE OF SERVICE

I, Brian T. Ross, an attorney, hereby certify that on December 3, 2018, I caused a true and correct copy of the foregoing instrument to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the court's CM/ECF System.

/s/ Brian T. Ross
Brian T. Ross
GIBBS & BRUNS LLP
1100 Louisiana, Suite 5300
Houston, Texas 77002
Phone: (713) 650-8805
E-mail: bross@gibbsbruns.com